

### **Amendments to the Claims**

The listing of claims will replace all prior versions, and listings, of claims in the application.

#### **Listing of Claims:**

1. (Currently Amended) A method of protecting memory locations associated with an embedded system, the method comprising:
  - starting a write filter that intercepts writes to the protected memory locations and stores the writes in a cache;
  - starting a state machine with at least a change state and a normal state;
  - upon starting the state machine, entering the change state when an indication is present that data needs to be persisted to the protected memory locations, otherwise entering the normal state;
  - in the normal state, identifying requests for critical writes to the protected memory locations and creating at least one update file in unprotected memory locations not protected by the write filter which describe describing the critical writes, wherein the critical writes are not persisted to the protected memory locations during the normal state; and
  - in the change state, applying the critical writes described in the updated file at least one update file and rebooting the system in a manner that persists the critical writes to the protected memory locations.
2. (Original) A method, as set forth in claim 1, further comprising:
  - emptying the cache upon startup of the embedded system.
3. (Currently Amended) A method, as set forth in claim 1, further comprising:
  - running applications of the embedded system in the normal ~~stat~~ state; and
  - not running the applications of the embedded system in the change state.

4. (Currently Amended) A method, as set forth in claim 1, wherein the step of applying the changes in the update file and rebooting comprises:  
determining whether the application of the changes was successful;  
if the application of the changes was not successful, deleting ~~the~~ the update files, erasing the indication, issuing a command to ~~empty~~ empty the ~~each~~ cache, and ~~rebooting~~ rebooting the embedded system; and  
if the application of the changes was successful, issuing a command to persist the cache, deleting the update files, erasing the indication, and rebooting the system.

5. (Previously Presented) A method, as set forth in claim 1, further comprising:  
in the normal state when an update file is created, creating an indication that data needs to be persisted to the protected memory locations.

6. (Original) A method, as set forth in claim 5, wherein the step of creating an indication comprises writing the file name of the update file to a data file.

7. (Original) A method, as set forth in claim 1, wherein the step of creating an update file further comprises naming the update file using a time stamp.

8. (Original) A method, as set forth in claim 1, further comprising:  
in the change state, if an update executable exists running said update executable.

9. (Original) A method, as set forth in claim 8, further comprising:  
putting the state machine in a sleep mode during the execution of the update executable.

10. (Previously Presented) An embedded system comprising:

US Patent Application Serial No. 10/630,031  
Docket No. 10030673-1

a processing unit responsive to an operating system for executing applications to perform the functions of the embedded system;

a main memory location storing the operating system of the embedded system, said operating system providing a write filter that protects the operating system from writes;

a secondary memory location for storing software and data; and

a control program that executes automatically upon booting of the system, said control program causing the embedded system to operate in a normal state and a change state, wherein:

during operation in the normal state, the applications are run and when a critical write to the operating system is requested, the critical write is not persisted to the operating system but an update file is generated in the secondary memory location to store the critical write until the embedded system enters the change state; and

during operation in the change state, no applications are run and the update file is used to update and persist the operating system.

11. (Currently Amended) An embedded system, comprising a state machine that in conjunction with booting assumes one of two states, the two states comprising:

a normal state ~~in which~~ wherein applications are executed ~~and, wherein~~ a write filter intercepts writes to a protected memory location and redirects them to a non-protected memory location, wherein the writes to the protected memory location are not applied to the protected memory location during the normal state, wherein critical writes to the protected memory location are identified and described in at least one update file located in non-protected memory; and

a change state, entered across a boot from the normal state, in which respective writes applied to the write filter during the last normal state are re-applied to the write filter and subsequently persisted to the respective protected memory locations, and wherein the critical writes described in the at least one update file are persisted to the protected memory.

starting a write filter that intercepts writes to the protected memory locations and stores the writes in a cache;

starting a state machine with at least a change state and a normal state;

upon starting the state machine, entering the change state when an indication is present that data needs to be persisted to the protected memory locations, otherwise entering the normal state;

in the normal state identifying requests for critical writes to the protected memory locations and creating at least one update file describing the critical writes, wherein the critical writes are not persisted to the protected memory locations during the normal state; and

in the change state, applying the critical writes described in the ~~updated~~ file update file and rebooting the system in a manner that persists the critical writes to the protected memory locations

12. (Currently Amended) A An embedded system, as set forth in claim 11, wherein applications are not run during the change state.

13. (Currently Amended) A An embedded system, as set forth in claim 11, wherein only critical writes are applied to the write filter and persisted in the change state.

14. (Currently Amended) An embedded system, as set forth in claim 11, wherein during the change state updates to an operating system of the embedded system are applied and persisted.

15. (Currently Amended) A An embedded system, as set forth in claim 11, wherein critical writes include writes to a system registry.

16. (Currently Amended) A An embedded system, as set forth in claim 11, wherein writes intercepted by the write filter in the normal state are copied to

at least one update file and in the change state the at least one update file is used as the source for re-applying the write to the write filter.

17. (Canceled).

18. (Currently Amended) A An embedded system, as set forth in claim 11, wherein the changes state is entered subsequent to a boot when indicators of updates are present.

19. (Currently Amended) A An embedded system, as set forth in claim 11, wherein ~~these~~ once all respective writes applied of the write filter during the last normal state have been persisted, the state machine enters the normal state.

20. (Currently Amended) ~~The~~ An embedded system, as set forth in claim 11, wherein the protected memory location stores an operating system of the embedded system.